PRIVACY IMPACT ASSESSMENT

International Parental - Child Abduction System (IPCA)

1. Contact Information

PIA Completed By: Name: Joyce France Title: PIA SME/IAE Org: CA/CST/ST Phone: 703-639-0384 Email: FranceJM@state.gov	**System Owner:** Name: Gerald L. Pascua Title: CA/CST Deputy Director and System Owner Org: CA/CST Phone: 202-485-7721 Email: PascuaG@state.gov
Program Manager: Name: Sharon B. Westmark Title: Program Manager Org: CA/CST/PSDD Phone: (202) 485-7722 Email: WestmarkSB@state.gov	**IT Security Manager:** Name: Edward F. Bacon Title: IT Security Branch Chief/CA ISSO Org: CA/CST/ST/S Phone: (202) 485-7813 Email: BaconEF@State.gov
A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services	

2. System Information

(a) Name of system: International Parental - Child Abduction System (IPCA)

(b) Bureau: Consular Affairs (CA)

(c) System acronym: IPCA

(d) iMatrix Asset ID Number: 39

(e) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒Yes

☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance – in routing for approval

(b) What is the security Assessment and Authorization (A&A) status of the system?

The system is currently undergoing its Assessment and Authorization (A&A) in order to receive an Authorization to Operate (ATO) status. IPCA is expected to receive an ATO by Spring 2021.

(c) Describe the purpose of the system:

The International Parental - Child Abduction System (IPCA) tracks information about international parental child abductions, denial of access, and abduction prevention from the initial stage through final resolution. The system tracks all documents, correspondence, and legal proceedings, and allows journal entries to be tracked by caseworkers. The Bureau of Consular Affairs Overseas Citizens Services Directorate, Office of Children's Issues (CA/OCS/CI) at the Department of State assists parents, attorneys, other government agencies, and foreign governments in the prevention and resolution of international parental child abduction cases. CA/OCS/CI is responsible for the management and tracking of information related to international parental child abduction cases and potential cases, including their related subjects, action items, legal proceedings, documents and notes.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

IPCA collects the following information on U.S. citizens and non-U.S. citizens:

- Name
- Phone number
- Email address
- Address
- Date of birth
- Place of birth
- Nationality
- Social Security Numbers
- Gender
- Physical description (height, eye and hair color)
- Passport Information
- Visa information
- Marital status
- Family information
- Arrests and criminal information
- Legal information

- IPCA collects the following business contact information from U.S. government employees and Institutions/Agencies working on abduction cases: name, work title, address, email and phone number. Examples of individuals in this category include legal offices, adoption agencies, Department of State employees assigned to the cases, and other personnel of other government agencies who may be involved.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 8 U.S.C. 1101 et seq., Immigration and Nationality Act of 1952, as amended, including 8 U.S.C. 1104 Powers and duties of Secretary of State and 8 U.S.C. 1185, Travel Documentation of Aliens and Citizens
- 18 U.S.C. 911, 1001, 1541-1546 Crimes and Criminal Procedure
- 18 U.S.C. 1073 – Fugitive Felon Act
- 18 U.S.C. 1204 –International Parental Kidnapping Crime Act (IPKCA)
- 22 U.S.C. 211a-218, 2705; Passports and Consular Reports of Birth Abroad of a U.S. Citizen
- 22 U.S.C. 1731 – Protection of Naturalized Citizens
- 22 U.S.C. 2651a Organization of Department of State
- 22 U.S.C. 2670j Provision of emergency medical, dietary and other assistance
- 22 U.S.C. 3904 Functions of service
- Executive Order 11295 of August 5, 1966, 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 22 CFR Subchapter F, Nationality and Passports, including 22 CFR 51.28, Minors Subchapter H, Protection and Welfare of Americans, Their Property and Estates; Subchapter J, Legal and Related Services, including Part 94, International Child Abduction
- 28 U.S.C. 1738A – Parental Kidnapping Prevention Act (PKPA)
- 42 U.S.C. 5779 Reporting Requirement and 42 U.S.C. 5780 State Requirements (National Child Search Assistance Act of 1990)
- 22 U.S.C. 9001 et seq – International Child Abduction Remedies Act (ICARA)
- 22 U.S.C. 9101 et seq – International Child Abduction Prevention and Return

(f) **Is the information searchable by a personal identifier (e.g., name or Social Security number)?**

☒Yes, provide:

- SORN Name and Number: STATE-26 Passport Record; STATE-05 Overseas Citizens Services Records and Other Overseas Records
    - SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): March 24, 2015; September 8. 2016

☐No, explain how the information is retrieved without a personal identifier.

(g) **Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?** ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) **Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system?** ☒Yes ☐No

(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:

A-13-001-12a: Passport Records Access and Disclosure Request Files
Description: Case files created in response to requests for information (Passport Records) under the Freedom of Information Act (FOIA), Mandatory Declassification Review (MDR) process, Privacy Act, Classification Challenge, and similar access programs: Includes requests (either first-party or third-party); replies; copies of requested records; administrative appeals; related supporting documents (such as sanitizing instructions).
Note 1: Record copies of requested records remain covered by their original disposal authority, but if disposable sooner than their associated access/disclosure case file, may be retained under this item for disposition with that case file.
Note 2: Agencies may wish to retain redacted copies of requested records for business use after the rest of the associated request case file is destroyed.

Disposition: Temporary. Destroy 6 years after final agency action or 3 years after final adjudication by courts, whichever is later, but longer retention is authorized if required for business use.
DispAuthNo: DAA-GRS-2016-0002-0001 (GRS 4.2, item 020)

A-15-002-1: General Policy Files (Abduction and Adoption)
Description: Memorandums, correspondence, telegrams, court decisions, briefing papers, and other matters handled by the Office of Childrens Affairs.

Disposition: Permanent. Cut off files when 10 years old and transfer to Records Schedule Center for transfer to the Washington National Records Center (WNRC). Transfer to the National Archives when 25 years old.
DispAuthNo: N1-059-97-14, item 1

A-15-002-02: Child Custody/Abduction Case Files

Description: Cases reflect applications filed for the return of children abducted to countries that are party and not party to The Hague Abduction Convention. Included are requests for assistance in locating children taken by the other parent, legal proceedings, information of available courses of action, monitoring the welfare of a child, information on child custody laws and procedures in the host country, and related correspondence.

Disposition: Transfer to the RSC after the case is deemed closed and no action has taken place for 1 year for transfer to the WNRC. Destroy when 15 years old.
DispAuthNo: N1-059-97-14, item 2

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system?
Please check all that apply.

☒ Members of the Public (are US citizens or aliens lawfully admitted for permanent residence)
☒ U.S. Government/Federal employees or Contractor employees
☒ Other (are not U.S. Citizens or aliens lawfully admitted for permanent residence)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒Yes ☐No

- If yes, under what authorization?

- Immigration and Nationality Act of 1952, as amended (8 U.S.C. 1101 et seq.):
- Title 22 U.S. Code Foreign Relations and Intercourse (various Chapters)
- Title 22 Code of Federal Regulations (CFR) (various parts, including, Parts 40 – 53 and Parts 96-99.)
- 26 U.S.C. 6039E (Information Concerning Resident Status)

(c) How is the information collected?

IPCA is an internal tracking database of information collected by CA/OCS/CI case workers by various means e.g., face-face, attorneys, foreign governments, court records, email, etc., and entered into the system manually. IPCA maintains information on U.S. citizens, non-U.S. citizens, and U.S. government employees. IPCA maintains the same information on children and parents involved in an international abduction, regardless of the child's citizenship status. Information is initially collected from the left behind parent (LBP). Once a case is opened, the information is supplemented with legal documentation from the LBP and/or their attorney, foreign governments, court records, family members, and/or non-governmental organizations via Consular Affairs records (passport, visa, and American Citizens Services) and various communication means such as phone, fax, email, face-to face. The CA/OCS/CI caseworker then gathers relevant information from law enforcement sources and international databases on the taking parent (TP) and missing child. All data are stored in the IPCA database. The system is only accessible by Department of State users.

(d) Where is the information housed?

☒ Department-owned equipment
☐ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other
- If you did not select "Department-owned equipment," please specify.

(e) What process is used to determine if the information is accurate?

IPCA's information is based upon information provided to the Department of State (DoS) representative by persons involved in international parental child abduction and access cases. Accuracy of the information is the responsibility of the person submitting the information. The information can be updated as the case progresses to closure. If information needs to be updated for accuracy while the case is open, a parent, legal representative, U.S. or foreign government entity, or other involved person would notify the CA/OCS/CI employee providing assistance, who can update the system.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

IPCA's information is based upon information provided to the Department of State representative by victims of international parental child abductions and missing children. The data are current when the information is provided and are updated as the case progresses to closure. If information needs to be updated while the case is open, the parent/legal representative would notify the caseworker providing assistance, who can update the system. After the case is closed, there is no need to update the information.

(g) Does the system use information from commercial sources? Is the information publicly available?

Yes, information regarding a child's location may be sought through commercial databases containing publicly available information, such as Lexis-Nexis. .

(h) Is notice provided to the individual prior to the collection of his or her information?

No, notice is not provided to the individual since IPCA is not public-facing nor does it collect information directly from individuals.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☐Yes ☒No

- If no, why are individuals not allowed to provide consent?

IPCA is not public-facing and is not accessed by the public. Consent is not required for this system which is accessed only by authorized Department of State personnel with access to IPCA.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The PII items listed in Question 3d are the minimum necessary to perform the actions required by this system to effectively address international parental child abduction and access cases. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by

users and/or a security breach. These risks were considered during the system design and security configuration.

5. Use of information

(a) What is/are the intended use(s) for the information?

The intended use of the PII in IPCA is to support the State Department's work on international parental child abduction and missing children cases and to provide related services to U.S. citizens. The information collected is used to validate identity of parents, abducted children, and others associated with the case; to locate parents, children and others who may be involved; and to acquire legal and criminal information to assess individuals' backgrounds during the processing of the cases.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes. The PII is used according to the purpose of the system, which is to support the State Department's work on international parental child abduction and access cases and to provide related services to U.S. citizens.

(c) **Does the system analyze the information stored in it?** ☐Yes ☒No

IPCA does not analyze the information. Rather, it generates reports that may be analyzed by Department of State authorized users processing international parental child abduction and international adoption cases.

Reports are used to review and document the details of a specific case. Routine statistical reports are generated on total counts of abduction/access cases by country for use by the Overseas Citizens Services Directorate (CA/OCS) management, CA/OCS/CI Abduction Unit and Department of State principals. The information is also used to produce annual reports required by Congress containing statistical information on international parental child abductions.

(1) Does the analysis result in new information? ☐Yes ☒No

(2) Will the new information be placed in the individual's record? ☐Yes ☒No

(3) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☒No

6. Sharing of Information

(a) **With whom will the information be shared internally and/or externally?** Please identify the recipients of the information.

Internally: The term "internal sharing" traditionally refers to the sharing of information within the Department of State (DoS), but external to the owning organization (referred to as "bureau"

at DoS). However, since the various Bureau of Consular Affairs (CA) offices have unique processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the bureau.

With that understanding, information in the IPCA system will be shared internally with the other CA systems, specifically the Consular Consolidated Database (CCD) and the Consular Shared Tables (CST).

Externally: Information stored in IPCA may be shared manually (not by system connection) with external law enforcement, foreign governments, Congress, other federal agencies such as the Federal Bureau of Investigation (FBI), and non-governmental organizations associated with child abduction cases to help locate or facilitate the return of an abducted child. The information collected in IPCA is also shared with the International Criminal Police Organization (INTERPOL), and foreign governments as the cases progress and collaborations with other legal and governmental entities become necessary.

Note: The IPCA information used by external entities are in accordance with relevant statutory authority and purpose, such as the National Child Search Assistance Act of 1990 (NCSA), specifically, 34 U.S.C. § 41307 (Reporting Requirement) and 34 U.S.C. § 41308 (State Requirements). The NCSA requires local, state and federal law enforcement agencies, when informed of an abduction, to immediately enter the appropriate data into the National Crime Information Center (NCIC) database without requiring a waiting period. Sharing the information that is necessary to help locate an abducted child with relevant law enforcement agencies is a "routine use" under SORN STATE-05, and is permitted under the NCSA.

(b) What information will be shared?

The PII listed in paragraph 3d is shared to perform the function for which it was intended, i.e., providing services in international parental child abduction cases. IPCA data are stored in the CCD database (outside the IPCA boundary) where an IPCA lookup report can be accessed by authorized individuals.

(c) What is the purpose for sharing the information?

The IPCA information is shared internally and externally with individuals who have a need-to-know because they are participants in the process of addressing or resolving international parental child abduction and access cases.

Internally: Information is shared internally within the State Department to allow employees to perform their functions. For example, U.S. Missions overseas may conduct welfare and whereabouts visits with abducted children and/or liaise with foreign governments in an effort to resolve cases.

Externally: Information shared with external agencies includes the whereabouts of parents and abducted children as needed by U.S. domestic and foreign law enforcement organizations. U.S. domestic and foreign child welfare NGOs or lawyers representing either parent require information regarding case status and case decisions. Applications for return of children are transmitted to the appropriate foreign central authorities charged with assisting in international

parental child abduction cases. Information is provided to these entities by officials acting on behalf of the Department of State via emails, letters, phone calls, in-person meetings or diplomatic notes.

(d) The information to be shared is transmitted or disclosed by what methods?

The internal Department of State IPCA information shared with CCD and CSTs is database to database. External sharing of information is by paper, secure email, phone calls, letters, in-person meetings, and diplomatic notes.

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal: Numerous management, operational, and technical controls are in place to reduce and mitigate the risks associated with internal sharing of information and disclosure including, but not limited to, annual security training, separation of duties, least privilege assignments and personnel screening

Communication between IPCA, CCD and CSTs is transmitted using Hypertext Transfer Protocol Secure (HTTPS) protocols and is encrypted using Secure Socket Layers (SSL). The Department of State's network security controls include firewalls and Network Intrusion Detection Systems (NIDS) which limit the risk of unauthorized access.

External: Data shared with other government agencies manually outside IPCA are carefully regulated according to a Memoranda of Understanding/Agreements (MOU/MOA) or other documents agreed to by Authorizing Officials of each Agency.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Privacy concerns regarding the sharing of information focus on two primary sources of risk:

a. Accidental disclosure of information to non-authorized parties
b. Deliberate disclosure/theft of information regardless whether the motivation was monetary, personal or other.

Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

These risks are mitigated using a multi-faceted approach to security:

- Frequent security training for all State Department personnel and contractors regarding information security, including the safe handling and storage of PII, "Sensitive but Unclassified", and all higher levels of classification, and signing a user agreement.

- Strict access control based on roles and responsibilities, authorization and need-to-know.

- System authorization and accreditation process along with continuous monitoring (Risk Management Framework (RMF)). Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

- All communications shared with external agencies are encrypted to protect the data prior to transmission.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

IPCA is not a public-facing system and does not obtain information directly from applicants. The public or parents do not have access to the IPCA system. They can access information by contacting the Department of State representative in the Overseas Citizens Services Directorate (CA/OCS), or by following procedures outlined in SORN STATE-26 Passport Records or SORN STATE-05 Overseas Citizens Services Records and Other Overseas Records.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

IPCA does not obtain information directly from applicants. Persons with PII in IPCA must contact the Overseas Citizens Services Directorate (CA/OCS) if CA/OCS has records pertaining to them in accordance with SORN STATE-05 and SORN STATE-26. The Department of State Travel.State.Gov website also provides contact information on the Child Abduction Frequently Asked Questions page as well as guidance on how to correct information.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?

Individuals are notified of the procedures to correct records in these systems by a variety of methods:

The CA/OCS/CI employees, SORN STATE-26, and SORN STATE-05 provide information to individuals on how to correct their information. In addition, the Department of State website at Travel.State.Gov provides contact information on the Child Abduction Frequently Asked Questions page as well as guidance on how to update and correct information.

8. Security Controls

(a) How is the information in the system secured?

The IPCA system is secured within the Department of State intranet, where risk factors are mitigated through the use of defense in-depth layers of security including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform official duties.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

Access to IPCA is limited to authorized users of the system, including civil service personnel and cleared contractors who have a justified need for the information in order to perform official duties. Authorization to the network requires a background investigation and an application approved by the supervisor and local Information System Security Officers. Each authorized user must agree to the rules of behavior before given a user account. Authorized users are issued a Personal Identity Verification /Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon.

The IPCA system is configured according to the State Department Security Configuration Guides to optimize security while still providing functionality. Applicable National Institute of Standards and Technology (NIST 800-53) security and privacy controls and overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities are noted during testing and are reported and tracked until compliant or acceptably mitigated.

Access to IPCA is role based, and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports that are to be restricted. Local Information System Security Officers (ISSOs) determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

The CA System Manager and CA Information System Security Officer (ISSO), in conjunction with the CA Security team, periodically scan and monitor information systems for compliance with Department of State Security Configuration Guides, and conduct annual control assessments (ACAs) to ensure that all systems/applications comply and remain compliant with Department of State and federal policies. Additionally, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor the network-connected systems that host CA's major and minor applications.

Access control lists on all Department of State servers and devices along with Department of State Security Configuration Guide Standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures. Remote

connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities.

In accordance with Department of State Security Configuration Guides, auditing is enabled to track the following events on the host operating systems, and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges and changes in file access restrictions.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

(d) **Explain the privacy training provided to the authorized users of the system.**

In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness Training, which has a privacy component, to access or use systems. All Department of State personnel are also required to take the course PA318 Protecting Personally Identifiable Information biennially.

Additionally, the Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require users to agree to the rules to protect PII through appropriate safeguards to ensure security, privacy and integrity.

(e) **Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users?** ☒Yes ☐No
If yes, please explain.

To combat the misuse of information by personnel, numerous management, operational and technical controls are in place in accordance with NIST 800-53 and Department of State Security Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Data in transit are encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, and incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to firewalls, intrusion detection systems, antivirus software, and access control lists are in use. System and information integrity auditing are implemented to monitor and record possible attempts at unauthorized access. All access to Department of State systems require dual factor authentication utilizing PIV/CAC and PIN.

(f) **How were the security measures above influenced by the type of information collected?**

Exposure of an individuals' PII may lead to inconvenience, distress, damage to standing or reputation, threats to personal safety, and financial loss. Security measures are in place to

minimize these risks, and to minimize the risk of harm to State Department programs or the public interest through an unauthorized release of sensitive information. The security measures listed above in paragraph 8(a-e) are implemented to secure the data in the system in compliance with federal laws and policies, including Department policies.

9. Data Access

(a) Who has access to data in the system?

IPCA users include Department of State IPCA users and Database and System administrators. Users are both civilian and contractor cleared personnel.

IPCA users – Department of State CA/OSC/CI employees and authorized contractors manage active abduction cases and maintain a central repository on all documentation relating to an open case.

Database Administrator - Database Administrators (DBA) are responsible for the daily maintenance, upgrades, patch/hot fix application, backups and configuration, to the database.

System Administrator - The System Administrators manages the system including its operating system and applications.

(b) How is access to data in the system determined?

Access is role-based and users are granted only the role(s) required to perform officially assigned duties. Role-based access requests are approved by the supervisor and local ISSO.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

Information is documented in the System Security Plan. The IPCA System Security Plan includes procedures regarding system access to data.

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Only administrators have access to all data in the system. Separation of duties and least privilege is employed and IPCA users have access to only the data that the supervisor and local ISSO approves to perform official duties.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

-Access control policies and access enforcement mechanisms control access to PII.

-Separation of duties is implemented.

-Least Privileges are restrictive rights/privileges or accesses needed by users for the performance of specified tasks. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

- Users are uniquely identified and authenticated before accessing PII via dual factor authentication utilizing a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon.